Août / Oct. 2013

LES CAHIERS DU HACKER

PIRATE // 18

[INFORMATIQUE]

100% NOUVELLE FORMULE...

Le GUIDE du PIRATE

EXPLOSIF

DES DIZAINES DE FICHES PRATIQUES

... ET TOUJOURS 0% CENSURE

ANONYMAT • MULTIMÉDIA • HACKING • SURVEILLANCE

BIG BROTHER
PRISM : Ce que la NSA sait de vous

ANONYMAT
Strealthy VS SoftEther : proxy contre VPN

TÉLÉCHARGEMENT
MEGA
6 mois après : le bilan et nos astuces

SOMMAIRE

PROTECTION/ANONYMAT

08-10
SOFTETHER : un VPN collaboratif gratuit et simple

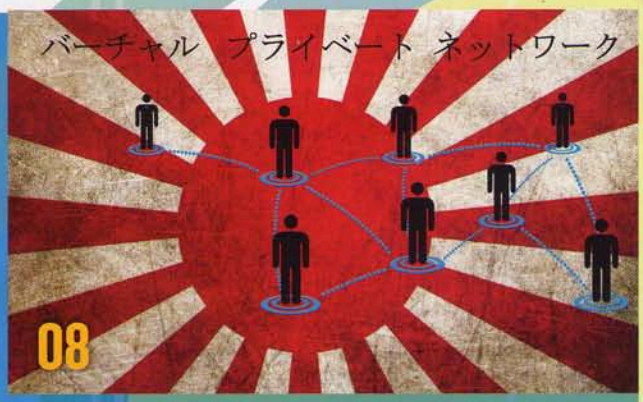
12-13
Changez d'IP comme de chemise avec **STEALTHY** et sa sélection de proxy

14-15
Blindez votre **SESSION WINDOWS** avec notre sélection de trucs & astuces

16-17
En local ou par Internet, nos meilleures solutions pour **TCHATTER** en toute sécurité

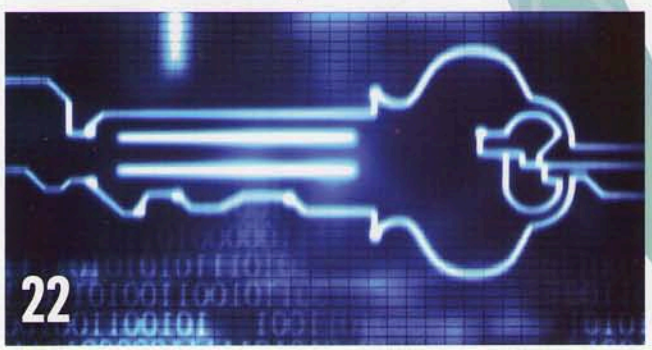
18-19
COBIAN BACKUP : des sauvegardes simples et paramétrables

20-21 MICROFICHES



HACKING

22-23
TRUPAX : le chiffrement pour les nuls !



24-25
BITMESSAGE : une messagerie cryptée pour Monsieur Tout-le-Monde

26-27
Manipulez les pages Internet et donnez-leur un peu plus de piquant avec **GREASEMONKEY**

28
MULTISKYPE LAUNCHER : qui a dit qu'il était impossible de lancer deux sessions Skype en même temps ?

30-31
CRYPTSYNC : cryptez les documents qui sont dans votre «Cloud» et tenez la CIA éloignée !

32-33 MICROFICHES

MULTIMÉDIA

35-37
MEGA : le point sur le successeur de MegaUpload

38
BITTORRENT SURF : Le plugin qui va (enfin) vous permettre de télécharger des Torrents depuis votre navigateur

40-41
Du stream illimité avec PureVid et MixtureCloud grâce à **MÉTÉO DÉBRIDEURS**

42-43
Trois solutions pour le **TORRENT À DISTANCE** : µTorrent, Vuze et Phrozen

44-45 MICROFICHES

BRICOL'HACK

46-49
Découvrez la présentation du **RASPBERRY PI** ainsi que notre premier projet pratique : la réalisation d'un Media Center HD pour moins de 55 €

+ NOTRE TEST

50-51
> NOTRE SÉLECTION DE MATÉRIELS

LES CAHIERS DU HACKER
PIRATE INFORMATIQUE

N°18 – Août / Octobre 2013

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication : David Côme
Le roi fou : Benoît BAILLEUL
Jon Snow : Pierre Corbinais
Tyrion Lannister : Yann Peyrot
Stannis Baratheon : Sergueï Afanasiuk
Daenerys Targaryen : Karima Allali

Imprimé par / Printed by :
ROTIMPRES - C/ Pla de l'Estany s/n
Pol. Industrial Casa Nova

17181 Aiguaviva - Espagne
Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS : Marseille 491 497 665
Capital social : 2000,00 €
Parution : 4 numéros par an.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.

ÉDITO

Choses promises, choses dues.
La nouvelle version de *Pirate Informatique* que vous être en train de tenir est la synthèse des souhaits que vous nous avez formulés ces dernières semaines. Une maquette plus claire, une nouvelle rubrique *Bricol'Hack* où nous réaliserons chaque mois un projet électronique ou de programmation ainsi que des microfiches classées par thématiques à la fin de chaque rubrique. Nous avons aussi réuni les parties *Anonymat* et *Protection* en une seule et même rubrique, car parfois la frontière entre ces deux thèmes est plutôt fine. Enfin, nous avons changé la formule du CD puisque vous étiez de plus en plus nombreux à désirer une galette en adéquation avec les articles du magazine à la place d'une simple compilation de logiciels.

Cette nouvelle formule tombe à point avec une actualité chargée. L'affaire Edward Snowden (voir page 6) a fait grand bruit, mais a donné raison à ceux qui protègent leurs documents et leurs communications. Ce numéro comporte donc toute une artillerie anti-CIA/NSA avec des pas à pas sur le chiffrement de niveau militaire, les VPN ou les messageries cryptées dans le but de protéger vos données. Bien sûr à chaque fois, nous expliquons tout en détail pour que la sécurité informatique et la protection de la vie privée ne soient pas réservées aux élites.

N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur benbailleul@idpresse.com

Bonne lecture !

Benoît BAILLEUL.

HACKTUALITÉS

Les enfants d'HADOPI

Il aura fallu un an à Pierre Lescure pour rédiger son rapport sur l'avenir d'HADOPI et sur les moyens de réconcilier le monde du numérique et une juste rémunération du monde de la Culture. Même si Monsieur Lescure est proche des milieux du cinéma et de la télévision, nous pensions qu'un homme de ce calibre aurait pu trouver des solutions ou au moins explorer des pistes nouvelles. Lorsque l'UFC-Que Choisir, suivi par La Quadrature du Net et un syndicat d'artiste ont décidé de snober la table ronde proposée par le créateur des *Enfants du rock*, nous nous sommes dit «*attendons de voir, pourquoi anticiper un fiasco ?*». Il faut dire qu'à la différence des associations précédemment citées, nous n'avions pas été invités à la réunion informelle qui précédait le début de sa mission (que voulez-vous, nous n'avons pas le poil soyeux d'un Jérémie Zimmermann). Et puis il paraît que quand quelqu'un a parlé de légalisation des échanges entre particuliers, Pierrot s'est braqué...

Le changement c'est du vent

Lorsque nous regardons le rapport, nous ne pouvons que tomber d'accord avec les boycotteurs. En premier lieu, HADOPI restera HADOPI même si les amendes remplaceront la suspension (inapplicable) de la connexion Internet. La notion de «négligence» est toujours dans la place. Il faudra donc toujours demander à Papy/Mamy de sécuriser eux-mêmes leur connexion Internet alors qu'ils peinent déjà avec Gmail.

Ensuite, la taxe sur les supports de stockage sera étendue à d'autres appareils comme les téléphones portables ou les NAS. Cette taxe, qui ne rend pas légale la copie, sera obligatoire même si vous n'avez qu'une sonnerie toute pourrie sur votre smartphone ou si vous utilisez votre serveur pour vos élèves. Attention, cette masse d'argent ne servira pas à aider de jeunes artistes à monter leurs spectacles ou concert, mais ira dans un fonds de soutien «*à la transition numérique des industries culturelles*». Bref, ça ira chez Universal et compagnie. Parmi les autres idées pourries, on compte le transfert de compétence de HADOPI vers le CSA (qui ne demande pas mieux que de mettre son grain de sel ici) ou encore le blocage de sites contrevenants sans être passé devant un juge. Comme quoi, choisir un mec avec une image «sympa» ne suffit pas.

MOURREZ EN PAIX avec Google

Vous ne vous êtes jamais demandé ce que deviendrait votre messagerie, votre espace de stockage ou les informations que vous avez en ligne le jour de votre mort ? Google a pensé à tout et propose maintenant de léguer votre compte Google à quelqu'un de confiance si vous veniez à disparaître. Appelé Gestionnaire de compte inactif, cette fonctionnalité, une fois activée, vous enverra un e-mail tous les X mois pour vous proposer de vous connecter. Au bout d'un laps de temps programmable, votre compte pourra être transféré vers un tiers (Gmail, Google+, YouTube, etc.) ou tout simplement effacé.

Merci à Korben.info !

Lien : **http://goo.gl/aqxCt**

Un peu de littérature !

Une fois n'est pas coutume, nous tenions à parler de deux livres dissertant d'Arduino. Rappelons qu'Arduino est un microcontrôleur électronique programmable permettant de faire mille et une choses : domotique, robotique, etc. Nous avions d'ailleurs réalisé deux articles complets dans les numéros 15 et 16 de *Pirate Informatique*. Édité par Elektor (qui est aussi l'éditeur du magazine d'électronique du même nom), *Maîtrisez les microcontrôleurs à l'aide d'Arduino* (de C. Valens à 38 €) et *Personnalisez vos montages Arduino* (de G. Spanner à 33 €) sont disponibles dès maintenant en suivant notre lien. Le premier s'adresse aux débutants tandis que le deuxième est destiné aux utilisateurs ayant quelques connaissances de base en électronique.

Lien: **www.elektor.fr/arduino**

LE CHIFFRE

1,5 MILLIARDS

C'est le nombre de mots de passe possible que le hacker Stun a compilé dans une grande base de données téléchargeable. Il a, non seulement, réuni les bases de données et dictionnaires de mots de passe, mais aussi les sésames les plus utilisés des dernières années ainsi que tous les mots contenus dans toutes les langues de Wikipédia. Le but est bien sûr de proposer un outil pour les amateurs de brute force [une technique qui consiste a essayer tous les mots de passe possible pour trouver le bon, NDLR]. Le tout pèse la bagatelle de 15 Go et compte 1,5 milliard de mots passes possibles. L'archive est disponible dans toutes les bonnes crèmeries et l'outil en ligne CrackStation a même été créé pour l'occasion...

Lien : **http://crackstation.net**

VU SUR INTERNET

PASCAL NÈGRE, L'HOMME QU'ON AIME DÉTESTER

Pascal Nègre, grand spécialiste du MP3 japonais (si, si !) et accessoirement PDG d'Universal Music France a encore fait parler de lui dernièrement. Encore une saillie drolatique sur le piratage ? Non cette fois, notre vendeur de soupe s'est attiré l'ire de toute la Twittosphère à cause de l'éloge funèbre de George Moustaki qu'il a envoyé sur le site de micro-blogging. Jugez plutôt :

Il n'en fallait pas plus pour que le petit monde d'Internet ne se moque gentiment de son petit billet. Un hashtag #TweetCommePascalNegre a même été créé. On y retrouve pêle-mêle des parodies du Tweet quelque peu maladroit :

-Mort de Amy Winehouse. -15 % chez Nicolas

-Le gamin de mes voisins est mort d'une leucémie. Retrouvez tous ses jouets à prix réduit sur leboncoin.fr

Notons au passage que Pascalou avait déjà fait la même chose lors des morts de Daniel Darc ou d'Henry Dutilleux. Aura-t-il compris le message cette fois ?

Lien : **http://goo.gl/Clvnp**

HADOPI SCORE ENFIN !

Lorsque HADOPI a été votée à la fin 2009, tous les médias avaient parlé de la sanction ultime de cette loi : la coupure de votre accès Internet au bout du troisième avertissement. Trois ans et demi après la mise en place des outils de surveillance, le bilan est plutôt morose pour HADOPI malgré les millions dépensé pour son fonctionnement : près de 2 millions de mails pour 30 transferts au parquet et seulement 3 personnes jugés (dont deux relaxés). Et les coupures dans tout ça ? Très difficile à mettre en place par le FAI, car si l'accès au Web doit bien être suspendu, la possibilité d'envoyer des e-mails, la TV et la téléphonie doivent être conservées. Pourtant, histoire de sauver l'honneur, un pauvre Internaute qui a téléchargé quelques chansons a été condamné à 600 € d'amende et 15 jours de suspension de sa connexion. Il s'agirait pourtant de la première et dernière coupure puisque Aurélie Filippetti, notre Ministre de la Culture a dernièrement parlé de supprimer par décret cette sanction. Le chant du signe pour HADOPI ?

Lien : **http://crackstation.net**

EN BREF...

LA CITATION

«Cela m'énerve à chaque fois que j'entends l'expression «interception légale» [mise sur écoute, NDLR] parce que la notion même d'interception légale indique que c'est OK, que c'est bien. Mais c'est des conneries. Ce n'est pas parce que c'est légal que c'est juste ou moralement justifiable. L'histoire a toujours été très dure avec ceux qui ont choisi de suivre la loi quand la loi était mauvaise.»

Rick Falkvinge, fondateur du Parti Pirate Suédois dans le documentaire *Une contre-histoire de l'Internet*.

Devenez mormon grâce à la CNIL

La CNIL (Commission Nationale Informatique et Liberté) est garante de la protection de nos données personnelles. C'est elle qui est censée éviter une utilisation abusive des données informatiques vous concernant. Or cette CNIL a décidé dans le plus grand silence de laisser la société Family Search International à mettre en œuvre un traitement automatisé de l'état civil français. Quand on sait que le but est l'extradition aux États-Unis de données sur nos ancêtres, on se pose des questions, mais quand on sait que derrière Family Search se cache L'Église de Jésus-Christ des saints des derniers jours (les mormons quoi) on s'en pose encore plus. Il faut savoir que les mormons ont comme hobby sacré de dresser l'arbre généalogique de l'humanité. Ces données serviront donc à cette tâche, mais aussi à baptiser à titre posthume certains de leurs aïeux Français. Non seulement la CNIL n'aura pas le pouvoir de vérifier la sécurisation une fois que les données seront à Salt Lake City, mais si nous devons devenir mormons, nous voudrions peut-être le faire de notre vivant ! Certes, il faudra que les généalogistes en herbes attendent 120 ans après le décès d'un individu pour obtenir ces informations, mais pourquoi la CNIL a-t-elle donné son accord ? L'Église est très riche, mais il s'agit avant tout de moyens. Les documents et microfilms sont en péril et l'Église a un certain savoir-faire ainsi que des milliers de bénévoles permettant de sauver ce patrimoine.

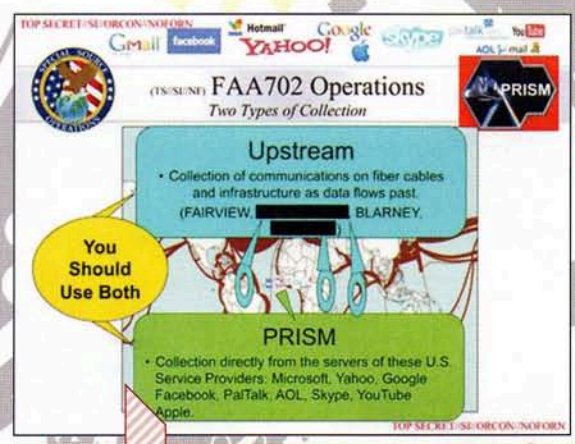
Merci à Zataz.com !

NSA : L'AGENCE QUI EN SAVAIT TROP

On s'en doutait, on en a maintenant la confirmation grâce aux documents fournis par l'ex-employé de la CIA et de la NSA, Edward Snowden : Les États-Unis ont accès à la totalité de nos communications, et ce, sans la moindre requête auprès des opérateurs ou des entreprises.

On savait que les géants du Web Google, Facebook, Microsoft et compagnie recueillaient nos données et conversations privées dans leur propre intérêt. On savait que la NSA (National Security Agency), encouragée par le Patriot Act et grâce au réseau Echelon, était capable d'intercepter n'importe quel appel ou e-mail en dehors des États-Unis. La seule chose que nous ne savions pas, c'est que ceux-là marchaient main dans la main.

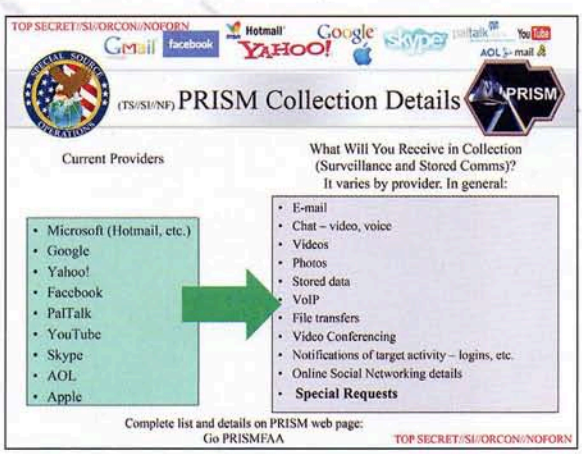
Des slides confidentielles de la NSA leakées par un de leurs administrateurs système, Edward Snowden, affirment en effet que Microsoft (dont Skype), Google (dont Gmail et YouTube), Yahoo!, Facebook, Paltalk (messagerie de type Skype), AOL et Apple autoriseraient l'agence de surveillance à explorer leurs serveurs sans la moindre requête ni le moindre mandat. C'est l'objet du programme sobrement intitulé PRISM.
Mais ce n'est pas tout ! D'autres révélations ont par la suite suivi : La NSA bénéficierait du même genre d'accord avec Verizon (une des plus grandes entreprises de télécoms américaines), qui lui fournirait un accès à toutes les informations d'appel de ses clients (heure, lieu, numéros, durée, numéro de série des mobiles...).
Enfin, c'est l'existence du «Boundless Informant» qui a été dévoilée, un outil filtrant les données sensibles par pays, et permettant ainsi de créer une carte des zones les plus à risque (ou les plus surveillées).



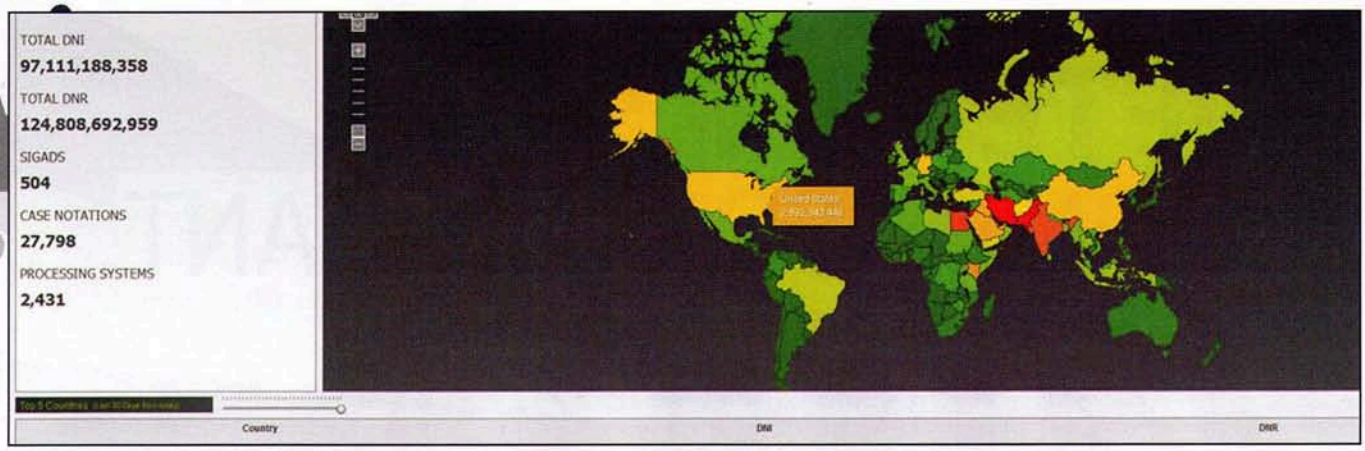
Slide extrait du diaporama du NSA. On y voit la distinction entre les interceptions de communication traditionnelles et le programme PRISM. *«Il faut utiliser les deux».*

Au Service de Sa Majesté

Si la NSA n'a pas réfuté la véracité de ces documents, les géants du Web ont, quant à eux, nié en bloc l'éventualité d'un accès direct à leur serveur. C'est pourtant bien ce qu'on peut lire sur les slides leakées : «*Collecte [de données] directement depuis les serveurs de ces fournisseurs de services américains*», en opposition aux flux de données interceptées par l'agence. On pourrait alors penser que par «accès direct», la NSA n'évoque pas de backdoors serveurs, mais un accès sur demande, comme l'affirment Google et compagnie, car, le Foreign Intelligence Surveillance Act et le Patriot Act imposent à toute entreprise américaine d'obéir aux requêtes du NSA sans poser de question et sans mandat ni justification nécessaire. Outre le fait qu'il s'agirait alors techniquement d'un accès indirect, pourquoi les «requêtes spéciales» sont-elles sur le diaporama, présentées comme un autre moyen de PRISM pour collecter les données ?
Quel que soit le véritable fonctionnement de PRISM, on peut tout de même affirmer



Slide extrait du diaporama du NSA. On peut y voir la liste des fournisseurs et celle des types de données récoltées.



avec certitude qu'aucune donnée hébergée chez Google, Facebook, Microsoft, Yahoo!, Apple, etc. n'est inaccessible à la NSA, celle-ci ayant la technologie comme la loi de son côté. Pensez-y la prochaine fois que vous uploaderez des photos personnelles sur Picasa ou des documents privés sur SkyDrive.

Ennemis d'état

Aussi choquantes que puissent être ces révélations, il faut bien reconnaître que cela ne change pas grand-chose pour nous, non-américains. Comme évoquée plus haut, la surveillance des communications mondiales par la NSA n'a rien de très nouveau, et les États-Unis ne sont pas vraiment connus pour leurs méthodes démocratiques en ce qui concerne la politique étrangère. Mais pour les Américains eux-mêmes, la donne a changée, car ceux-là ont eu l'occasion de constater qu'ils ne sont pas espionnés par la Chine ou quelque autre puissance, mais par leur propre gouvernement. Comble de l'ironie, le Boundless Informant montre que les États-Unis sont bien plus surveillés que la plupart des autres pays. Que les citoyens américains ne s'alarment pas, cependant, car le programme PRISM, selon les dires d'Edward Snowden, est conçu pour ne recueillir les données que s'il est certain à 51 % que la cible n'est pas l'un d'entre eux. 51 %, c'est un chiffre qui rassure, non ? Apparemment oui, puisqu'un sondage effectué par le Washington Post montre que 56 % des Américains feraient confiance à la NSA, et jugeraient cette surveillance utile pour lutter contre le terrorisme.

La Peur au ventre

Face au programme PRISM, la pensée de l'Américain moyen semble donc être *«si c'est pour notre sécurité alors ça va»*. Mais est-ce réellement une question de sécurité ? Suite aux révélations de Snowden, le directeur de la NSA a annoncé au Congrès américain que PRISM avait permis d'éviter *«des douzaines»* d'attaques terroristes. Avec près de 97 milliards d'éléments collectés par mois, quelques douzaines, ça semble bien la moindre des choses. Pourtant, quelques jours plus tard, le gouvernement américain envoie un communiqué aux homes politiques et journalistes, indiquant que le projet PRISM aurait servi à repousser *«au moins une»* attaque terroriste. Tout de suite, c'est moins impressionnant... d'autant plus que le gouvernement évoque l'attentat du métro de New York, qui d'après les documents judiciaires rendus publics, a en réalité été intercepté par Scotland Yard... On en arrive donc à ce moment gênant où ni le gouvernement ni la NSA ne sont capables de prouver l'utilité de PRISM d'un point de vue sécuritaire.

La Vie des autres

Mais si en fait PRISM servait à toute autre chose ? Et s'il ne s'agissait pas vraiment de surveillance ? Après tout, avoir accès à toutes les données stockées chez Google ou Microsoft par des compagnies étrangères pourrait s'avérer une aubaine en termes d'espionnage industriel. Pas étonnant alors d'apprendre de Snowden que plus de 61 000 opérations d'intrusion auraient été engagées par la NSA contre la Chine. D'autre part, difficile de croire que les presque 3 milliards d'éléments collectés sur le sol des États-Unis en un mois seulement concernent tout le terrorisme. PRISM pourrait tout aussi bien être une manière d'espionner activistes ou simples opposants politiques.

Il va falloir que les Américains s'y fassent : leur chère NSA est loin d'œuvrer pour le bien des citoyens. Nous ? On en était déjà convaincu, mais comme nous ne sommes pas rancuniers, nous allons faciliter le travail de tri de l'agence en chiffrant nos données.

LES PAYS LES PLUS SURVEILLÉS PAR LA NSA

D'après l'outil Boundless Informant

LES PLUS SURVEILLÉS

- Iran
- Pakistan
- Jordanie

MASSIVEMENT SURVEILLÉS

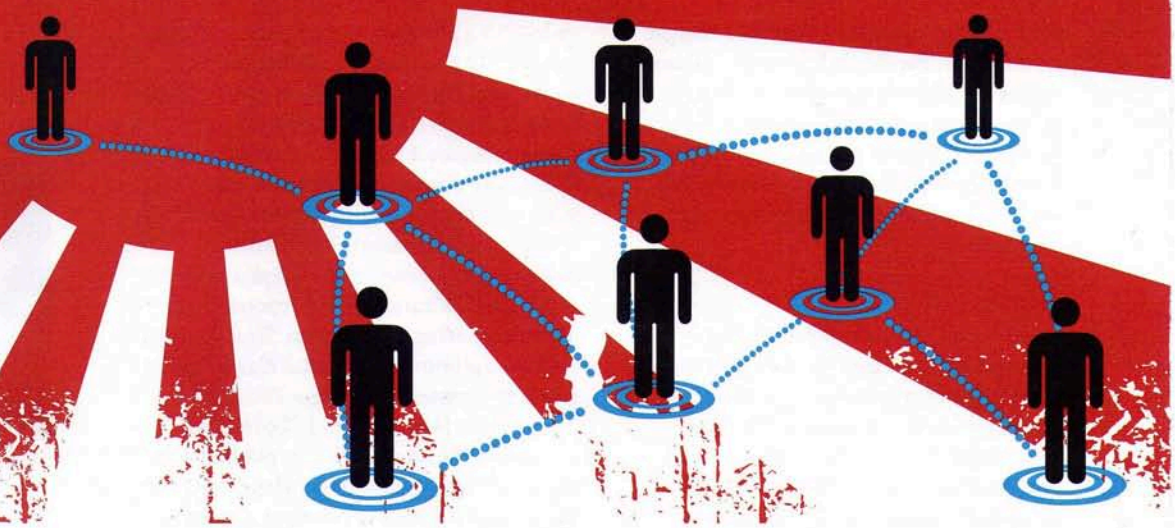
- Inde
- Égypte

TRÈS SURVEILLÉS

- États-Unis
- Chine
- Allemagne
- Arabie saoudite
- Irak
- Afghanistan
- Kenya

SOFTETHER : LE VPN DU SOLEIL LEVANT

バーチャル プライベート ネットワーク



À part quelques rares exceptions (comme nos amis de Freedom-IP), les VPN sont devenus des services commerciaux payants. Pour garder un certain anonymat sur Internet, il existe pourtant des solutions. Le projet SoftEther de l'Université de Tsukuba au Japon propose un réseau de relais chiffrés auxquels chacun peut se connecter ou participer à l'agrandissement...

LEXIQUE

***VPN :**
Virtual Private Network ou réseau privé virtuel. Il s'agit d'une connexion sécurisée entre ordinateurs via Internet. Le but est de recréer en ligne le même fonctionnement qu'un réseau local. Chiffré, personne ne peut savoir ce qui passe par les postes des utilisateurs connectés.

Se connecter à un VPN peut devenir vital dans certains pays. C'est en pensant aux citoyens surveillés et brimés en Chine, en Iran ou en Biélorussie que le projet SoftEther a vu le jour. Il s'agit d'un VPN basé sur un réseau de serveur «volontaire». Un internaute peut s'y connecter avec le logiciel client, mais aussi participer à l'agrandissement du réseau en devenant un serveur relais. Ces derniers ne pouvant pas être filtrés de manière efficace par les gouvernements censeurs proposent donc une «porte de sortie» aux citoyens pour consulter Internet sans restrictions, mais aussi commenter sur les blogs, forums ou poster sur Twitter, YouTube, etc.

CHIFFRÉ DE BOUT EN BOUT

À l'intérieur de ce réseau, tout est chiffré, mais très simple à employer puisque vous n'aurez pas à toucher à vos réglages de pare-feu grâce au protocole SSL-VPN. En utilisant ce dernier, il est possible de se connecter, de se déconnecter ou de changer de relais en un seul clic sans aller dans les entrailles de Windows pour configurer un à un les serveurs. Pour ceux ayant leurs petites habitudes (ou qui se connecterait sous Mac, voir l'illustration), pas moins de 6 protocoles sont acceptés (OpenVPN, IPsec, L2TP, MS-SSTP, L2TPv3 and EtherIP) en plus du SSL-VPN.

ANTI-DICTATURE MAIS PAS QUE...

Sans avoir forcément quelque chose à cacher ou habiter dans un pays qui pratique la censure, vous pouvez vous aussi trouver une utilisation à SoftEther. Il est, par exemple, possible d'avoir accès à des services multimédias comme Hulu ou Netflix sans pour autant être américain. Il suffit de se choisir un VPN aux USA ! De même, vous pouvez avoir accès aux services français (VoD, Replay TV) alors que vous êtes à l'étranger en prenant un serveur en France. Vous vous connectez souvent sur des réseaux Wi-Fi dont vous ne connaissez pas le degré de sécurisation ? Avec SoftEther, il devient impossible pour un pirate de s'introduire sur votre ordinateur ou d'usurper votre identité lorsque vous surfez sur le même réseau que lui (sidejacking).
Pour le téléchargement via P2P ? Cela marche aussi sous certaines conditions... Enfin si vous trouvez votre démarche un peu égoïste, vous pouvez vous aussi faire office de serveur relais pour les autres participants.

PAS À PAS

Se connecter avec SoftEther

CE QU'IL VOUS FAUT

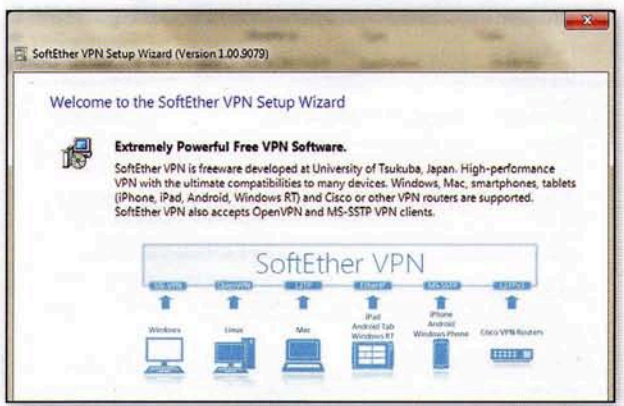
SOFTETHER

OÙ LE TROUVER ? :
http://goo.gl/8bZB7

DIFFICULTÉ : ☠☠☠

01 LA BONNE VERSION

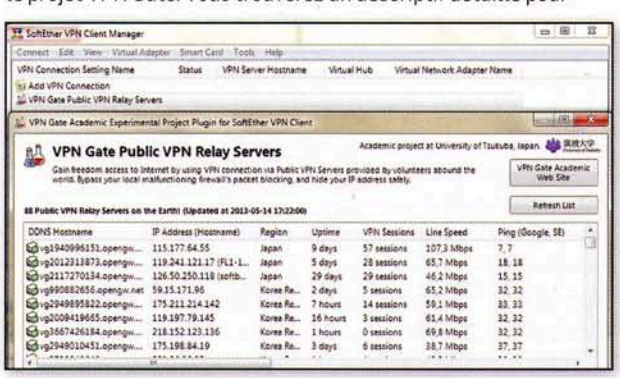
Il faudra dans un premiertemps télécharger la version de SoftEther qui comprend le plugin VPN Gate (suivez notre lien puis **Download SoftEther VPN Client + VPN Gate Client Plug-in**). VPN Gate

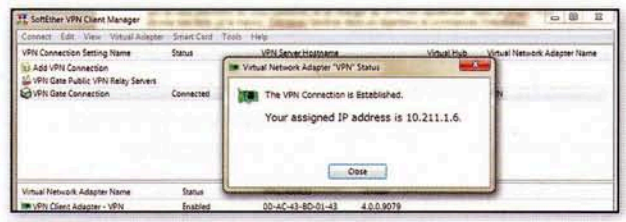


est un projet annexe de SoftEther qui va vous permettre de vous connecter et de changer de VPN très rapidement. Sans ce plugin, vous devrez tout faire «à la main»). Dézippez l'archive dans un répertoire et commencez l'installation. Sélectionnez **SoftEther VPN Client** lorsqu'on vous le demandera, acceptez les termes de la licence et cliquez enfin sur **Terminer**. Vous devriez voir l'interface principale du client.

02 LA LISTE DES SERVEURS «VOLONTAIRES»

Double-cliquez sur **VPN Gate Public VPN Relay Server** puis faites **OK** pour avoir une liste des serveurs disponible sur le projet VPN Gate. Vous trouverez un descriptif détaillé pour

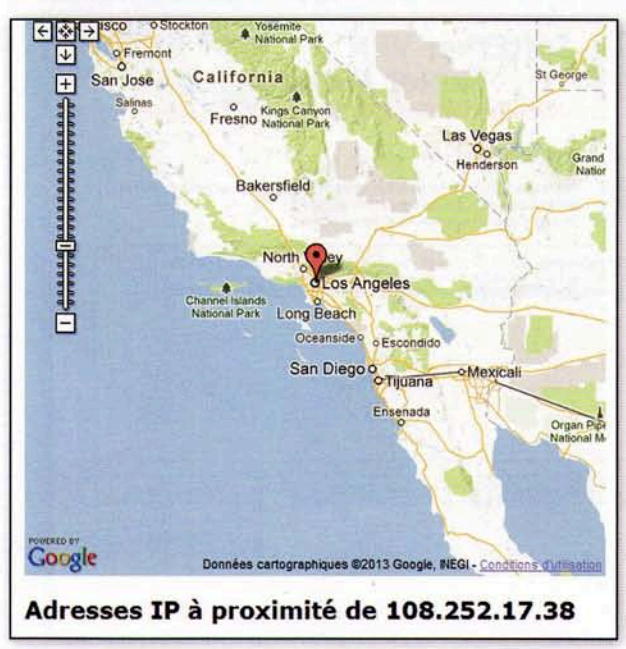




chacun d'eux: pays, ping, transfert cumulé, rapidité, nombre de personnes connectées et même une note finale pour faire son choix. N'habitant (pas encore) dans une dictature, mais voulant profiter de Hulu pour ses séries, nous allons choisir un VPN aux USA... Double-cliquez sur le serveur de votre choix. Faites **Agree** (après avoir coché **Do Not Show This Message Again**) et vous voici l'heureux propriétaire d'une nouvelle IP!

03 NOUVELLE IP + ÉCHANGES CRYPTÉS

En faisant un clic droit dans l'icône de la barre de notification, vous pourrez vous connecter automatiquement au démarrage. Si le VPN vous le demande, choisissez toujours l'option **Use TCP Protocol**. À vous les séries sur Hulu ou la possibilité d'avoir un compte Netflix. Et si vous êtes à l'étranger, on trouve aussi des serveurs français... Quant à la sécurisation d'un hotspot public, choisissez le VPN le plus proche et le plus rapide puisque de toute façon les échanges sont chiffrés. En allant sur **www.localiser-ip.com**, vous pourrez voir graphiquement votre nouvelle demeure virtuelle. Pour vérifier que le VPN masque aussi les échanges P2P, utilisez le site **Check my Torrent IP** que nous vous avons présenté dans le dernier numéro...



Adresses IP à proximité de 108.252.17.38

PAS À PAS

Créer un relais pour SoftEther

01 L'INSTALLATION

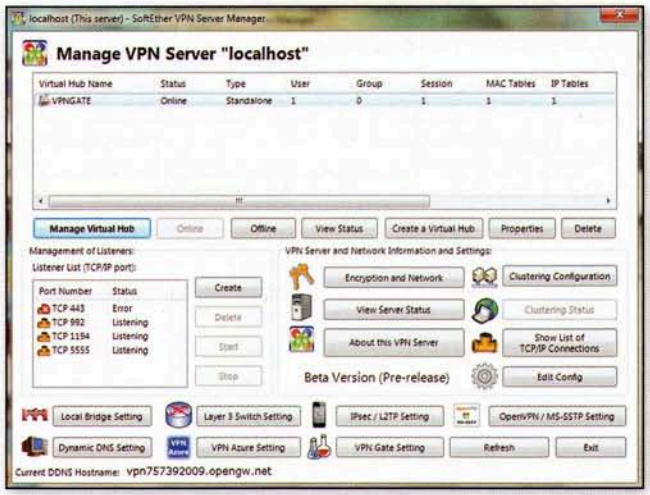
Vous profitez de SoftEther pour vous connecter, mais vous aimeriez participer à la nébuleuse? Pas besoin d'un serveur physique, un simple PC sous Windows suffit... Vous n'avez même pas à posséder les privilèges administrateurs! Bien sûr, tout cela est sécurisé et personne ne pourra vous pirater par ce biais. Commençons par télécharger et installer **SoftEther VPN Server and VPN Bridge**. Sélectionnez **SoftEther VPN Server** lorsqu'on vous le demandera et cliquez sur **Terminer** à la fin du processus.

02 VOTRE VPN PERSO

Dans la fenêtre qui s'affiche, sélectionnez **localhost (this server)**, faites **Connect** et paramétrez un mot de passe. Dans la fenêtre **Bidge Easy Setup**, cliquez sur **Close** sans cocher de case. Si le programme vous demande de configurer IPsec, dites **Non** (vous pourrez le faire plus tard). Le **SoftEther Server Manager** devrait alors s'afficher. En bas, cliquez sur **VPN Gate Setting** et cochez la case pour activer ce service dans la fenêtre qui s'affiche. Ne faites pas **OK,** mais allez plutôt dans **VPN Gate Service Option Settings...** Ici, vous devrez présenter votre relais avec votre nom, une adresse e-mail où vous joindre pour dénoncer un abus ainsi qu'un court message pour les utilisateurs. Cochez **Enable L2TP/IPsec VPN Server Fonction** et faites **OK** deux fois.

03 DES RÉGLAGES PLUS POUSSÉS

Ça y est! Vous faites maintenant parti des généreux volontaires offrant un accès aux internautes du monde entier! Dans **View Status,** vous pourrez voir le nombre de personnes connectées et bien plus. Il y a trop d'options pour faire le tour dans cet article, mais sachez que vous pouvez paramétrer le chiffrement dans **Encryption and Network** et que vous pouvez changer le nom de votre VPN dans **Dynamic DNS Setting**. À ce sujet d'ailleurs, le DNS dynamique est activé par défaut, mais si vous voulez placer votre VPN sur un serveur avec une IP fixe, il est possible de le faire en cliquant sur **Disable Dynamic DNS Function**. Pour des réglages plus pointus (prise de contrôle de votre VPN à distance, etc.), le site **www.softether.org** dispose de tutoriels dans sa partie **Documents**.



LE 1ER MAGAZINE
100% ANDROID ET 100% PRATIQUE

MINI PRIX
2,95 €
seulement

Chez votre marchand de journaux

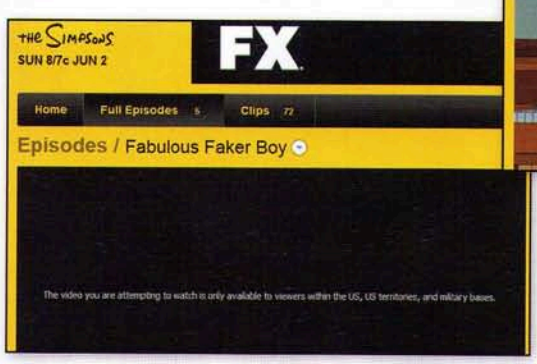
STEALTHY : SOYEZ FURTIF SUR LE NET

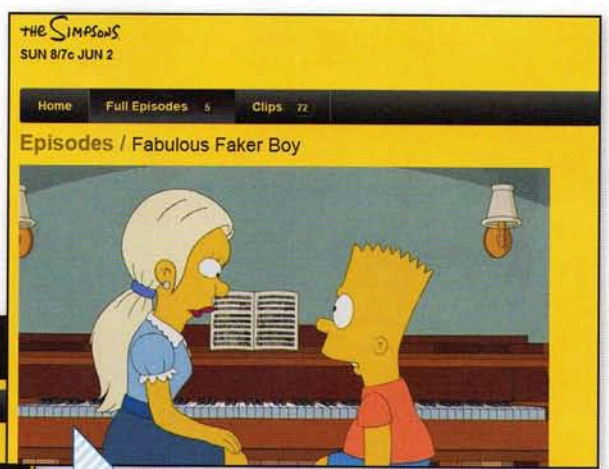
Pourquoi passer par un VPN si vous ne téléchargez rien ou que vous ne vous connectez jamais à un hotspot non sécurisé ? Les proxy permettent de masquer votre IP lorsque vous surfez, mais ils sont souvent difficiles à mettre en place pour les débutants. Avec Stealthy, plus de problème...

Stealthy est une extension pour Google Chrome et Firefox qui va vous permettre de masquer votre IP lorsque vous êtes sur Internet. Plus précisément, vous «empruntez» une IP autre que la vôtre : celle de votre proxy. Une fois connecté à ce serveur, les sites de stream ou les services en ligne qui exclue les internautes en fonction de leur position géographique (la radio en ligne Pandora, les sites de stream vidéo Hulu ou Netflix) ne pourront plus le faire puisque pour eux, vous serez résident américain. Vous pouvez aussi utiliser un proxy pour brouiller les pistes ou éviter le traçage des sites qui vous «fliquent».

UN TRAFIC «RE-ROUTÉ », MAIS PAS CHIFFRÉ

Il est assez fastidieux de saisir «à la main» les coordonnées d'un proxy à chaque fois que vous voulez vous connecter, mais heureusement Stealthy permet de réduire ces opérations à deux ou trois clics. Après l'installation, il suffit de choisir la destination de votre proxy, de mettre en route l'extension et c'est tout ! Attention, ce type de connexion ne fait pas passer l'ensemble de votre trafic, mais uniquement le HTTP qui permet de surfer ou de télécharger en direct (sans passer par un réseau P2P donc). De même, ils ne chiffrent pas les informations comme avec un VPN, attention donc à ce que vous faites transiter dans les «tuyaux»...





Le dernier épisode des Simpsons sur le site de la Fox. Sans Stealthy, un message vous avertit que vous devez être résident américain pour en profiter. Avec un proxy basé aux USA, pas de problème...

LEXIQUE

***PROXY :** En français, on parlera de serveur mandataire. Ce type de machine permet de faire le tampon entre votre ordinateur et Internet. Il existe des proxy permettant de se protéger ou de masquer son IP.

***EXTENSION (PLUGIN) :** Il s'agit d'un programme qui vient s'intégrer sur un autre programme pour lui ajouter des fonctions. La plupart des navigateurs proposent d'ajouter des plugins pour améliorer la sécurité, télécharger des Torrents ou traduire des pages. Ici, il s'agit d'anonymat.

***GÉOLOCALISATION :** Les sites Internet peuvent savoir de quel pays vous vous connectez grâce à votre IP. Certains services comme M6 Replay ou Pandora ne fonctionneront que dans leur pays d'origine. Stealthy permet de gruger le système en faisant croire que vous êtes résident américain ou français (lorsque vous êtes à l'étranger).

DEUX OPTIONS EXCLUSIVES POUR CHROME

La version Chrome de Stealthy intègre deux options assez sympathiques. La première est l'option incognito qui permet d'utiliser le proxy en mode de navigation privée (**Ctrl+Maj+N**). La deuxième permet d'exclure certains sites de la navigation avec proxy. Cela permet notamment de consulter votre Gmail, de faire une recherche sur Google ou de lire vos news sans pour autant peser sur la connexion et faire transiter votre trafic par l'autre bout du monde inutilement.

PAS À PAS

Mise en place de Stealthy

CE QU'IL VOUS FAUT

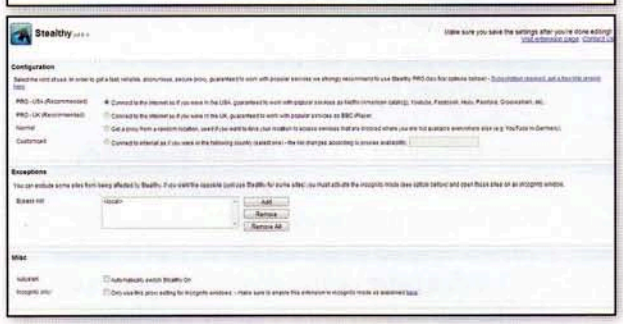
STEALTHY

OÙ LE TROUVER ? :
http://goo.gl/8bZB7

DIFFICULTÉ :

01 INSTALLATION

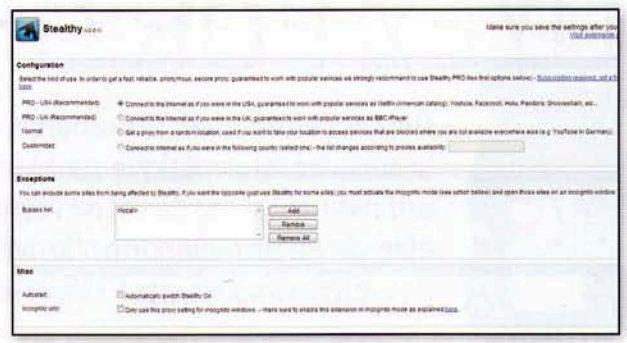
Allez sur le lien correspondant à votre navigateur et faites **Ajouter à Firefox**, **Installer maintenant** puis **Redémarrer maintenant** ou **Add to Chrome** et **Ajouter**. Vous serez alors



dirigé vers la page de Stealthy. Notez que le site propose un Webproxy permettant de naviguer anonymement. Néanmoins, ce dernier ne fonctionnera pas avec le stream. De même à certaines heures, vous devrez passer par la version payante de l'extension pour certains proxy.

02 LE CHOIX DU PROXY

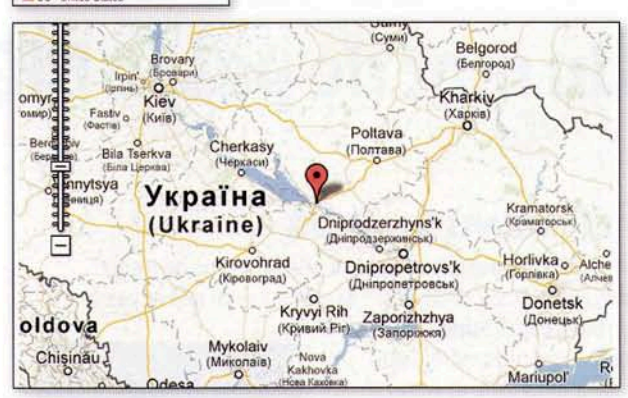
Vous aurez alors une nouvelle icône en haut à droite de votre navigateur. Pour les réglages, cliquez dans la petite flèche à droite de l'icône puis faites **Préférences** (pour Firefox) ou cliquez sur l'icône avec les troisbarres puis **Outils**>**Extensions** (dans Chrome). Vous aurez alors le choix de vous connecter à un proxy américain (pour éventuellement vous connecter à des services géolocalisés comme Hulu ou Netflix), un proxy anglais (pour le service de stream de la



BBC) ou à un proxy complètement au hasard (si vous êtes au Royaume-Uni et que vous voulez vous connecter à The Pirate Bay, interdit chez les sujets de Sa Majesté).

03 ACTIVATION

La dernière option permet de vous connecter à un proxy suivant le pays que vous désirez «emprunter». Tapez la premièrelettre de ce pays et choisissez-le dans la liste. Pour activer les réglages, il suffira de cliquer dans l'icône de Stealthy en haut à droite pour qu'elle devienne verte. Cela signifiera que vous êtes bien connecté. Vérifiez votre nouvelle «nationalité» en allant sur le site **www.localiser-ip.com**.



UNE SOLUTION ALTERNATIVE

Si les proxy vous intéressent, mais que Stealthy ne vous semble pas assez pointu pour votre utilisation, nous vous parlerons dans le prochain numéro de FoxyProxy. Cette extension pour Firefox permet de mémoriser et de jongler entre plusieurs proxy de votre choix. Et si vous ne savez pas où vous tourner pour trouver des proxy qui valent le détour, le site **www.idcloak.com** propose une liste mise à jour des meilleurs serveurs en fonction de leur niveau d'anonymat, de leur vitesse et du protocole utilisé...

BLINDEZ
VOTRE SESSION WINDOWS

Depuis ces derniers 18 numéros, nous avons traité à peu près tous les aspects de la sécurité informatique sans jamais aborder un sujet : l'accès physique à votre ordinateur. En cas de vol de votre PC ou d'intrusion à votre domicile, comment être sûr qu'un malandrin n'arrivera pas à récupérer vos données sensibles (mot de passe, documents, etc.) ? Voici nos pistes...

LEXIQUE

***BIOS :**
Pour Basic Input Output System. Il s'agit en fait du premier programme qui se charge lorsque vous mettez votre ordinateur sous tension. Il met en route les périphériques «primaires» comme les disques durs ou certains composants de la carte mère. Il met aussi en route Windows puisque c'est lui qui définit les priorités de «boot».

On a souvent du mal à l'imaginer, mais un ordinateur contient ou donne accès à bien des informations qui sont susceptibles de se retourner contre vous en cas de vols ou d'intrusion. En dehors des documents scannés présents dans votre disque dur comme les actes de naissance ou les pièces d'identité et qui peuvent être utilisés pour usurper votre identité, il existe aussi le piège des mots de passe enregistrés.

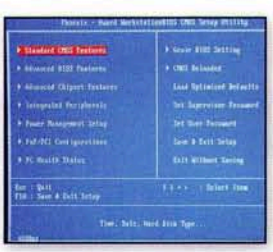
PENSEZ TOUJOURS AU PIRE !

En effet, les utilisateurs trop confiants laissent souvent leur navigateur mémoriser leurs sésames Gmail, Hotmail, Facebook, eBay ou PayPal. Cela ne pose pas de problème si votre brigand est incapable d'ouvrir votre session Windows, mais dans le cas contraire, il peut dévaliser votre vie privée en s'accaparant vos comptes en ligne, scruter vos fichiers joints, regarder vos conversations Skype, voler votre argent ou prendre «en otage» certains de vos comptes (restitution contre une somme d'argent). Il existe bien sûr des solutions pour contourner la saisie du mot de passe de Windows, mais en ajoutant diverses protections, vous n'aurez pas à vous inquiéter pour cela. Voyons donc comment ajouter un mot de passe au BIOS, ajouter un mot de passe Windows ou le changer si celui-ci est trop faible et faisons le point sur les autres méthodes pour protéger votre ordinateur...

PAS À PAS Un mot de passe BIOS

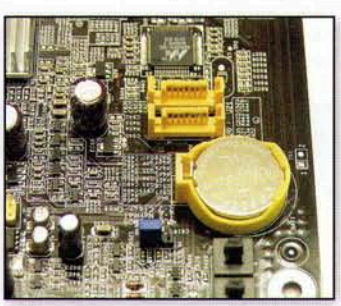
01 LE MENU DU BIOS

Cette méthode n'est pas infaillible, mais elle permettra de gruger les pirates débutants. Il s'agit en fait de configurer un mot de passe depuis le BIOS. Faites **Suppr** ou **F1** (en fonction de votre carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Ici, vous devriez trouver dans le menu une ligne du genre **Set User Password.** Ne confondez pas avec **Supervisor Password** (ou **Setting Password**) qui lui va protéger les réglages du BIOS et non l'accès à Windows. Validez avec **Entrée**, tapez le mot de passe de votre choix (éviter de mettre le même que celui de votre session Windows) et confirmer en le tapant une secondefois.



02 ATTENTION !

Il faudra parfois sauvegarder les changements avec une touche du clavier (cela dépend de votre carte mère). Ce mot de passe vous sera demandé avant même celui de Windows. Attention pour contourner ce mot de passe, il existe certains logiciels comme PC CMOS Cleaner. On peut aussi simplement retirer la pile plate CR2032 qui alimente la carte mère et permet de garder en mémoire l'heure et les réglages **Setup** du BIOS. Certains modèles disposent aussi d'un cavalier qui permet de réinitialiser le tout.

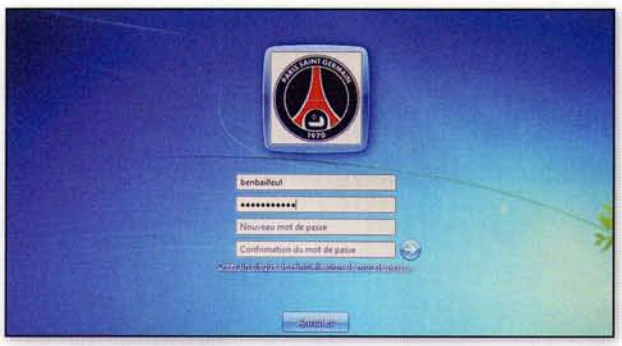


PAS À PAS

Mot de passe Windows et verrouillage de session

01 LE MOT DE PASSE

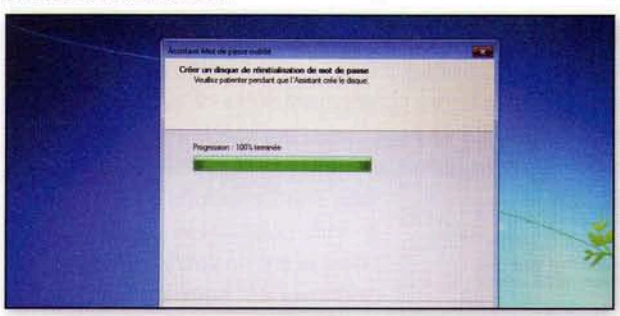
Si vous n'avez pas de mot de passe Windows, il est temps d'en mettre un. Même si cette fonctionnalité n'est pas infaillible, elle sera plus «coriace» que l'astuce du mot de passe BIOS.



Pour activer ou changer votre mot de passe Windows, faites **Ctrl**+**Alt**+**Suppr**, puis cliquez sur **Modifier le mot de passe**. Ici, il faudra taper votre ancien mot de passe (ne mettez rien si vous n'aviez pas de mot de passe jusqu'ici), puis le nouveau mot de passe (deuxfois). Validez avec **Entrée**.

02 VOTRE «FICHIER CLÉ»

C'est ici que vous pourrez créer un «fichier clé» au cas où vous oublieriez votre sésame. Cliquez sur la ligne **Créer un disque de réinitialisation de mot de passe** sans oublier de placer une disquette (une quoi?) ou de brancher une clé USB sur votre PC. Faite **Suivant** puis tapez votre mot de passe. Il faudra ensuite choisir la lettre de votre clé USB et valider. Un fichier **userkey.psw** va alors être créé sur votre lecteur. Cachez cette clé et utilisez-la en cas d'oubli.



03 VERROUILLAGE MANUEL

Une fois que votre mot de passe Windows est saisi et activé, il faudrait penser à paramétrer le verrouillage de votre session. En effet, pour l'instant Windows ne vous demandera le sésame qu'à l'allumage or, il arrive que vous vous absentiez alors que le PC reste allumé. Pour verrouiller votre session manuellement, il suffit de faire **Win** (la touche du clavier avec le logo Windows) + **L** puis d'entrer votre mot de passe pour revenir à votre bureau (cela n'éteint en rien vos programmes ou tâches actifs).

04 VERROUILLAGE AUTOMATIQUE

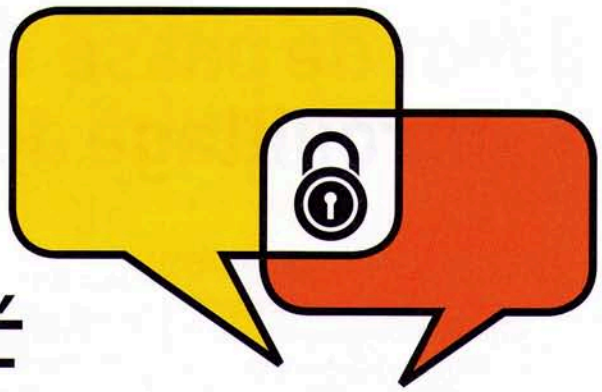
Pour verrouiller automatiquement sa session utilisateur en toute simplicité après tant de minutes d'inactivité, faites un clic-droit sur votre **Bureau** et sélectionnez **Personnaliser**. Cliquez ensuite sur **Écran de veille** puis choisissez **Aucun** dans la liste déroulante. Cochez ensuite **A la reprise, demander l'ouverture de session** et indiquez un temps en minute à gauche de cette dernière. Si vous ne touchez pas à votre clavier et souris pendant le nombre de minutes indiquées précédemment, votre ordinateur se verrouillera automatiquement.

LES DISPOSITIFS BIOMÉTRIQUES OU ÉLECTRONIQUES

Certains ordinateurs sont maintenant équipés de dispositifs de reconnaissance d'empreintes digitales, mais on en trouve aussi au format USB. Pratique, si on ne veut pas retaper son mot de passe 10 fois par jour. Et que diriez-vous si votre webcam vous reconnaissait ? Blink est un logiciel de reconnaissance faciale proposant d'ajouter une protection supplémentaire à votre authentification Windows. Il existe aussi des bagues électroniques qui permettent de verrouiller votre session lorsque vous vous éloignez de plus de 10 mètres de votre PC. Attention pour la plupart de ces dispositifs, le mot de passe Windows reste obligatoire en cas de panne ou de casse...

Lien : **www.luxand.com/blink**

TCHAT : PAPOTEZ EN TOUTE SÉCURITÉ



Pour bavarder avec ses amis, on peut se contenter de Skype (surtout depuis que ce dernier a fusionné avec MSN), mais pour s'échanger des messages confidentiels, il est plus dur de trouver un logiciel vraiment sécurisé. *Pirate Informatique* vous propose de découvrir deux programmes pour régler une fois pour toutes ce problème.

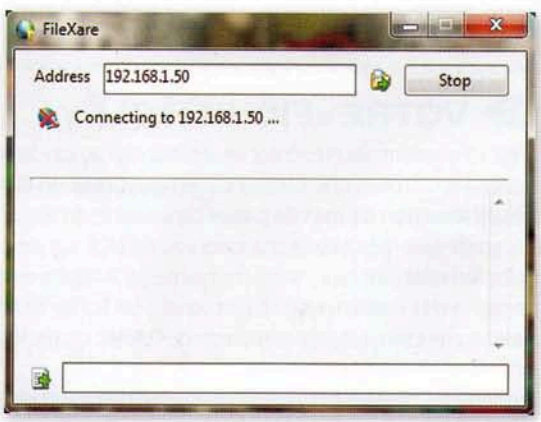
Si vous chiffrez vos e-mails, pourquoi ne pas passer à quelque chose de plus solide lorsqu'il s'agit de messagerie instantanée ? Si vous devez vous échanger des messages confidentiels pour éviter l'espionnage industriel, par exemple, la solution passe par des logiciels plus solides. En fonction de votre utilisation, nous vous avons trouvé deux logiciels plus adaptés aux professionnels que Skype, Google Talk ou Yahoo! Messenger.

TORCHAT, UNE MESSAGERIE CHIFFRÉE

TorChat est une messagerie qui va chiffrer de bout en bout vos communications. Tout est tunnelisé de votre IP au serveur qui héberge le service en passant par le contenu de vos messages. Comme Tor, qui permet de surfer en restant anonyme ou TorBirdy qui chiffre vos e-mails, TorChat protège votre identité et celle de vos correspondants. Il faut bien sûr échanger ses clés publiques avec vos collègues ou amis, mais une fois que c'est fait, vous pouvez bavarder incognito...

FILEXARE, EXCLUSIVEMENT SUR VOTRE RÉSEAU LOCAL

Et si vous travaillez sur le même réseau que tous vos correspondants ? Imaginez que vous souhaitiez communiquer avec vos collègues sans pour autant que vos messages passe



par Internet ? C'est possible avec FileXare. En utilisant simplement votre réseau local, ce dernier va vous permettre d'échanger textes, pièces jointes et même de converser à plusieurs. Vous économisez du temps, des e-mails et jamais vos messages ne sortiront de votre réseau. Si ce dernier est convenablement sécurisé avec du WPA, vous êtes totalement protégés.

Sur le Net ou en local, à vous de choisir la solution adaptée à vos besoins en matière de messagerie

LEXIQUE

***TOR :** Il s'agit d'un protocole inventé pour rendre anonyme ses intervenants sur Internet (pour contrer les espions ou les gouvernements)

***CHIFFREMENT :** Procédé qui consiste à rendre incompréhensible un fichier ou une communication. Le terme «cryptage» est toléré.